



Ciberseguridad para niños

Federico Basualdo

<https://www.linkedin.com/in/federicobasualdo/>



Que es la ciberseguridad?

- La ciberseguridad es la práctica de defender ordenadores, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques malintencionados. También se conoce como seguridad de las tecnologías de la información o seguridad de la información electrónica. El término se aplica en diversos contextos, desde la empresa a la informática móvil, y puede dividirse en algunas categorías comunes. (ESP-AR)

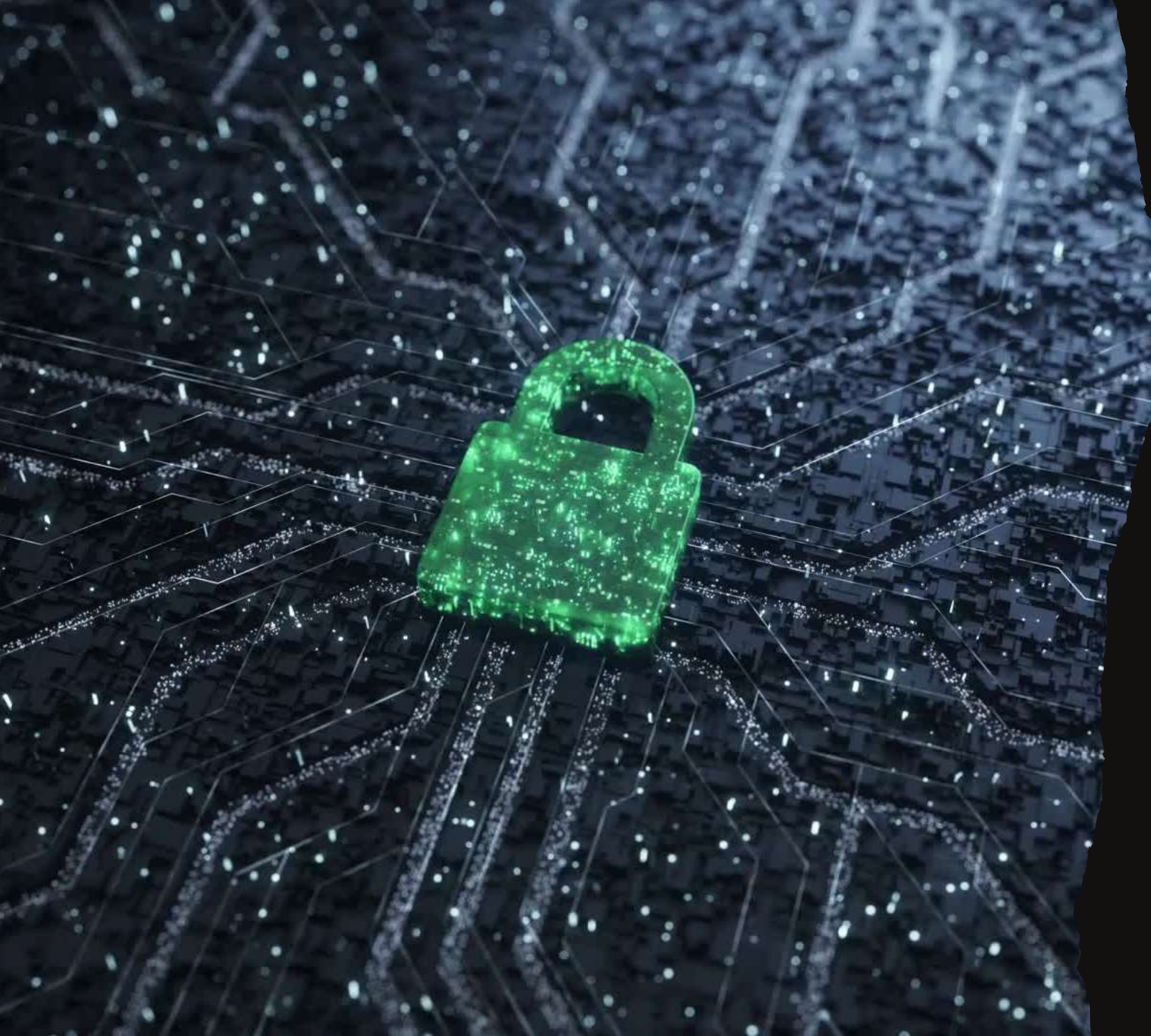
<https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>



Amenazas de seguridad en internet

- **Virus**: Tal vez la amenaza más conocida para la seguridad informática, un virus informático es un programa diseñado para alterar el funcionamiento de un ordenador, sin el permiso o el conocimiento del usuario. Un virus se replica y ejecuta a sí mismo, normalmente causando daños al ordenador en el proceso.
- **Hackers y depredadores**: Son las personas, y no los ordenadores, quienes crean los programas maliciosos y las amenazas a la seguridad informática. Los hackers y depredadores son programadores que victimizan a otros para su propio beneficio irrumpiendo en los sistemas informáticos para robar, alterar o destruir información como forma de ciberterrorismo. Estos depredadores online pueden comprometer la información de tarjetas de crédito, bloquear tus datos y robar tu identidad. Como habrá adivinado, las herramientas de seguridad en línea con protección contra el robo de identidad son una de las formas más eficaces de protegerse de este tipo de ciberdelincuentes
- **Phishing**: Haciéndose pasar por una persona o empresa de confianza, los “phisher” intentan robar información personal o financiera confidencial a través de correos electrónicos o mensajes instantáneos fraudulentos. Los ataques de phishing son algunos de los métodos más exitosos para los ciberdelincuentes que buscan una violación de datos.

<https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats>



Depredadores
Ciberneticos

- Internet es mucho más anónimo que el mundo real. La gente puede ocultar su identidad o incluso fingir ser alguien que no es. Esto puede representar a veces un peligro real para los niños y adolescentes que están en línea. Los depredadores en línea pueden intentar atraer a niños y adolescentes a conversaciones sexuales o incluso a encuentros cara a cara. A veces, los depredadores envían material obsceno o piden a los niños que envíen fotos de sí mismos. Por eso es importante que ***enseñe a sus hijos a estar en guardia siempre que se conecten a Internet.***
- Los adolescentes suelen estar más expuestos a los depredadores. Como son curiosos y quieren ser aceptados, ***pueden hablar con un depredador de buena gana***, aunque sepan que es peligroso. A veces, los adolescentes pueden creer que están enamorados de alguien en Internet, lo que les hace más propensos a aceptar un encuentro cara a cara.
- Aunque no es necesariamente probable que un depredador se ponga en contacto con su hijo, el peligro existe. A continuación, les comparto algunas pautas que puede dar a sus hijos para ayudarles a mantenerse a salvo de los depredadores en línea.
- **Evita utilizar nombres de usuario o fotos sugerentes.** Pueden atraer la atención no deseada de los depredadores en línea.
- **Si alguien te halaga en Internet, desconfía.** Aunque muchas personas en Internet son realmente agradables, los depredadores pueden utilizar los halagos para intentar iniciar una relación con un adolescente. Esto no significa que tengas que sospechar de todo el mundo, pero debes tener cuidado.
- **No hables con nadie que quiera entrar en temas demasiado personales..** Si quieren hablar de cosas sexuales o personales, debes poner fin a la conversación. Una vez que te metes en una conversación (o en una relación), puede ser más difícil parar.
- **Ten en cuenta que las personas no siempre son quienes dicen ser.** Los depredadores pueden hacerse pasar por niños o adolescentes para hablar con ellos en Internet. Pueden utilizar una foto de perfil falsa y añadir otros detalles para parecer más convincentes.
- **Nunca concierte una cita con alguien que haya conocido en Internet.** Los depredadores pueden intentar quedar cara a cara con un niño o adolescente. Aunque la persona parezca simpática, puede ser peligroso.
- **Si encuentras algún problema, díselo a uno de tus padres o a un adulto de confianza..** Si alguien te hace sentir incómodo en Internet, díselo inmediatamente a uno de tus padres o a un adulto de confianza. También debes guardar los correos electrónicos u otras comunicaciones porque pueden ser necesarios como prueba.



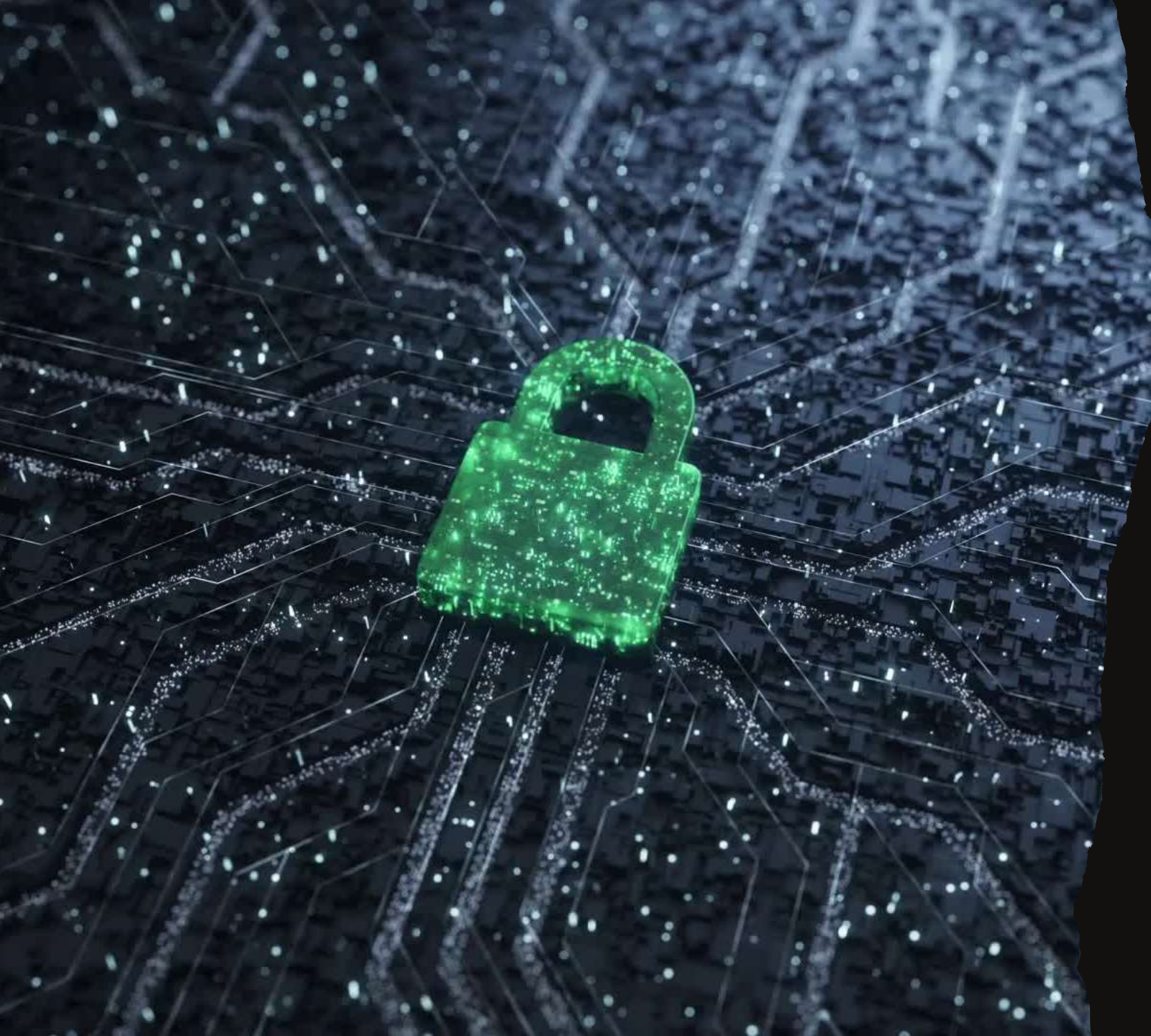


- **Con quién ponerse en contacto si hay un problema**
- Si cree que su hijo está siendo contactado por un depredador en línea, solicite ayuda inmediata a los siguientes recursos:
- **Policia local:** si su hijo está en peligro inminente, debe llamar al 911. Si no, puede llamar al número de no emergencias de la policía local para denunciar un problema.
- Medios digitales para denunciar un delito en Internet si la policía local no dispone de recursos suficientes, como comisarías especializadas en ciberdelincuencia.

A background image of a library aisle with tall wooden bookshelves filled with books. A hand is holding an open book in the foreground, slightly out of focus. The text 'Links de ciberdepredadores' is overlaid on the right side of the image.

Links de ciberdepredadores

- <https://www.youtube.com/watch?v=6jMhMVEjEQg&>
- https://www.youtube.com/watch?v=DFWjf5_O-fk
- <https://www.youtube.com/watch?v=euc-WcN5IkY&t>
- https://www.youtube.com/watch?v=dbg4hNHsc_8
- <https://www.youtube.com/watch?v=xk4VmYrquAs>
- <https://www.youtube.com/watch?v=m6Z7EWFTYTU&t>



Cyberbullying



- Al igual que los depredadores ya no tienen que salir de casa para interactuar con los niños, los acosadores ya no tienen que estar cara a cara con sus víctimas. El ciberacoso a través de las redes sociales es, por desgracia, frecuente en el mundo actual y causa tanto daño como cualquier otra forma de acoso. Puede decirse que es una de las amenazas más difíciles de afrontar, aunque una solución es evitar que sus hijos creen perfiles en las redes sociales. Hazles saber que pueden crear los suyos cuando sean mayores. Si no quiere hacerlo, recuerde a sus hijos que siempre pueden acudir a usted si sufren acoso, ya sea en línea o no. No podrás hacer mucho a menos que sepas que está ocurriendo en primer lugar.
- La gran mayoría, el 90%, de los adolescentes está de acuerdo en que el ciberacoso es un problema, y el 63% cree que se trata de un problema grave. Es más, una encuesta de 2018 sobre el comportamiento en línea de los niños descubrió que aproximadamente el 60% de los niños que utilizan las redes sociales han sido testigos de algún tipo de acoso y que, por diversas razones, la mayoría de los niños ignoraban por completo este comportamiento. Y según enough.org, en febrero de 2018, casi la mitad (47%) de los jóvenes habían sido víctimas de ciberacoso. Las redes sociales y los juegos en línea son el patio de recreo virtual de hoy en día, y ahí es donde tiene lugar gran parte del acoso cibernético, y funciona las 24 horas del día, los 7 días de la semana. Los niños pueden ser ridiculizados en los intercambios de las redes sociales. O, en los juegos en línea, sus personajes pueden ser objeto de ataques incessantes, convirtiendo el juego de una aventura imaginativa en un calvario humillante que se convierte en ciberacoso a través de múltiples plataformas y en la vida real.
- La mejor base para protegerse contra el ciberacoso es hablar con los hijos sobre lo que ocurre en sus vidas en Internet y en la vida real, y sobre cómo enfrentarse a los acosadores. Los programas de ciberseguridad y las aplicaciones especializadas para vigilar la actividad móvil y en línea de sus hijos pueden ayudar, pero nada sustituirá a un diálogo abierto.

A hand is holding an open book, showing its pages. The book is being held in front of a large library with many wooden bookshelves filled with books. The shelves are curved, and the books have various colored spines. The lighting is bright, and the overall atmosphere is that of a quiet library.

Cyberbullying Links

- <https://www.youtube.com/watch?v=GSE6spm-gyl>
- <https://www.youtube.com/watch?v=xAk8FqRFXy0>
- <https://www.youtube.com/watch?v=Ne9rPuoNi9w>
- <https://www.youtube.com/watch?v=vmQ8nM7b6XQ>
- <https://www.youtube.com/watch?v=i1oF5pXq2bc>
- https://www.youtube.com/watch?v=t8Lf_hcuJk
- <https://www.youtube.com/watch?v=CZ0YzebcBxw>
- <https://www.youtube.com/watch?v=mWQoikd72A4>
- https://www.youtube.com/watch?v=f6K9le_Chjs
- <https://www.youtube.com/watch?v=pHtnr7wkN7E>
- <https://www.youtube.com/watch?v=Y9D2PFD7nTI>
- <https://www.youtube.com/watch?v=E0WbSOplIqY>
- https://www.youtube.com/watch?v=eQo-Tkxnl_I
- <https://www.youtube.com/watch?v=asTti6y39xl>
- <https://www.youtube.com/watch?v=LC1BYXkHG3A>



Informacion
Personal



- Los niños aún no entienden los límites sociales. Pueden publicar **información personal identificable (IPI)** en línea, por ejemplo, en sus perfiles de redes sociales, que no debería ser pública. Puede tratarse de cualquier cosa, desde imágenes de momentos personales incómodos hasta la dirección de su casa o sus planes de vacaciones familiares.
- Gran parte de lo que publican sus hijos, aunque no todo, es público. Esto significa que usted también puede verlo, y no está de más recordarles que si mamá y papá pueden verlo, también lo puede ver todo el mundo. Evite espiar, pero hable francamente con sus hijos sobre los límites públicos y lo que significan para ellos y para toda la familia.



Informacion Privada links

- <https://www.youtube.com/watch?v=opRMrEfAlil>
- <https://www.youtube.com/watch?v=TyVM-H9P1RI>
- <https://www.youtube.com/watch?v=9XebSJxJYuo>
- <https://www.youtube.com/watch?v=1DmoMR-oX6o>
- <https://www.youtube.com/watch?v=yYFOCKq8WA4>
- <https://www.youtube.com/watch?v=PIIMsykXqLk>

Cyber Bullying Victims



Amanda Todd

🇨🇦 1996-2012



Phoebe Prince

🇮🇪 1994-2010



Ryan Halligan

🇺🇸 1989-2003



Tyler Clementi

🇺🇸 1991-2010



Megan Meier

🇺🇸 1992-2006

www.nobullying.com



Sexting



¿Qué es el sexting?

- El sexting es el envío de mensajes, fotos o vídeos sexualmente explícitos a través del teléfono móvil, el ordenador o cualquier dispositivo digital. El [sexting](#) incluye fotos y vídeos que contienen desnudos o muestran actos sexuales simulados. También incluye mensajes de texto en los que se habla de actos sexuales o se proponen.
- A medida que los adolescentes y los niños llevan cada vez más teléfonos inteligentes y utilizan tabletas, redes sociales, aplicaciones y mensajería, el riesgo de que envíen o reciban contenido sexual explícito se ha convertido en una preocupación para padres, profesores y fuerzas del orden.
- El sexting suele ser una broma, una forma de llamar la atención o de coquetear. Los padres deben hablar del tema con sus hijos para asegurarse de que entienden los riesgos y qué hacer si se les presiona para que participen.



¿Por qué es un problema el sexting?

- Una foto compartida entre dos personas puede convertirse rápidamente en un fenómeno viral. Los adolescentes pueden creer que se mantendrá en privado y luego descubrir que se ha compartido ampliamente con sus compañeros, a veces con graves consecuencias. Entre ellas, las detenciones de adolescentes que han compartido fotos suyas o de otros adolescentes menores de edad.
- Aunque algunos estados tienen leyes que diferencian el sexting de la pornografía infantil, otros no. El sexting puede dar lugar a acusaciones de distribución o posesión de pornografía infantil.
- La intimidación, el acoso y la humillación son problemas comunes cuando las fotos y los mensajes se comparten más allá del destinatario previsto. Puede haber graves consecuencias emocionales y sociales, como el suicidio de adolescentes cuyas fotos se han compartido.



¿Cómo pueden los padres prevenir el sexting?

- Inicie la conversación antes de que su hijo tenga un incidente. Si va a regalar a su hijo un teléfono inteligente o una cámara web, es el momento de hablar del sexting. También puede utilizar noticias o argumentos de programas de televisión o películas para iniciar la conversación.
- Lo mejor para hablar del sexting es hacerlo sin prejuicios y de forma informativa. Mantener el diálogo abierto deja espacio para que tus hijos hablen contigo en lugar de esconder las cosas. Además, tenga en cuenta que los niños pueden tener un nombre diferente para el sexting, por lo que tendrá que ser claro sobre el tema que está discutiendo.

A background image of a library aisle with tall wooden bookshelves filled with books. A hand is holding an open book in the foreground, with its pages slightly blurred. The lighting is warm and the perspective is looking down the aisle.

Sexting Links

- <https://www.youtube.com/watch?v=PL57cjJlp7g>
- <https://www.youtube.com/watch?v=MoRtLk1xihY>
- <https://www.youtube.com/watch?v=SuBxI5OGdlw>
- https://www.youtube.com/watch?v=uFKAfo_etkE
- <https://www.youtube.com/watch?v=RWxAimnKupE>
- <https://www.youtube.com/watch?v=UPgHh3wOusI>
- <https://www.youtube.com/watch?v=oAl2ajdDirk>
- <https://www.verywellfamily.com/what-is-sexting-problem-1258921>
- <https://www.webmd.com/sex/what-is-sexting>



Sobreexposicion
en redes sociales



- Si cada vez estamos más dispuestos a exponer nuestras vidas en las redes sociales y compartir todo tipo de momentos y situaciones, no necesariamente tenemos que abandonar la prudencia para pensar y elegir qué publicar, dónde publicar y, sobre todo, para quién publicar. La sobreexposición, conocida mundialmente como **Oversharing**, es difícil de medir, pero siempre podemos partir del sentido común y de una reflexión sobre el contexto en el que compartimos algo.
- Todos somos libres de compartir cosas de nuestra vida con los demás, pero no podemos olvidar las diferencias de exposición dentro y fuera de la red. Si en un viaje en autobús o avión, o incluso en la cola de un banco, no nos sentimos cómodos compartiendo y exponiendo parte de nuestra intimidad con desconocidos, entonces sabemos que no es todo tipo de contenido el que podemos exponer, tanto por nuestra seguridad como para no avergonzar a la otra persona.
- En Internet hay que tener el mismo cuidado, sumado a algunas diferencias importantes porque todo, todo lo que compartimos queda registrado y perdemos el control total sobre quién puede tener acceso a ese contenido. Ya no somos los únicos propietarios de una información que puede ser utilizada no sólo por los sitios que alojan las páginas y los servicios, sino por usuarios de todo el mundo que pueden buscar y encontrar estos detalles sobre nuestras vidas muy fácilmente si nos excedemos en la exposición online. Y, como siempre, la información sobre nuestra intimidad sacada de contexto puede perjudicarnos, tanto ahora como en el futuro.

A hand is holding an open book, showing its pages, in a library aisle. The shelves are filled with many colorful books, and the perspective is looking down the aisle. The background is slightly blurred, emphasizing the book being held.

Overexposing Social Network Links

- <https://www.youtube.com/watch?v=0EFHbruKEmw>
- <https://www.youtube.com/watch?v=e2xm5fc5MQk>
- <https://www.youtube.com/watch?v=tRo9n8M7zIE>
- <https://www.youtube.com/watch?v=Zbqo7MGVElw&t>
- <https://www.youtube.com/watch?v=KdtPNRzuKrk>
- <https://www.youtube.com/watch?v=Y6oUf81b1OI>
- <https://www.youtube.com/watch?v=0hs8rc2u5ak>
- <https://www.youtube.com/watch?v=aP8yrkkLWIM&t>



Phishing



- [Phishing](#) es como llaman los profesionales de la ciberseguridad al uso de correos electrónicos que intentan engañar a la gente para que haga clic en enlaces o archivos adjuntos maliciosos. Estos pueden ser especialmente difíciles de detectar para los niños porque, a menudo, el correo electrónico parecerá provenir de alguien legítimo, como un amigo o un familiar, diciendo simplemente: "¡Eh, pensé que te gustaría esto!". Esto también puede hacerse con el uso de aplicaciones de mensajería o mensajes de texto, entonces se llama "smishing". (Smishing es un ataque que utiliza la mensajería de texto o el servicio de mensajes cortos (SMS) para ejecutar el ataque. Una técnica común de smishing consiste en enviar un mensaje a un teléfono móvil a través de SMS que contenga un enlace en el que se pueda hacer clic o un número de teléfono de retorno).



5 COMMON TYPES OF PHISHING



EMAIL PHISHING

Scammers create emails that impersonate legitimate companies and attempt to steal your information.



SPEAR PHISHING

Similar to email phishing, but the messages are more personalized. For example, they may appear to come from your boss.



CLONE PHISHING

Scammers replicate an email you have received, but include a dangerous attachment or link.



WHALING

Scammers target high-ranking executives to gain access to sensitive data or money.



POP-UP PHISHING

Fraudulent pop-ups trick users into installing malware.

Email Phishing

- El correo electrónico de phishing básico es enviado por estafadores que se hacen pasar por empresas legítimas, a menudo bancos o proveedores de tarjetas de crédito. Estos correos electrónicos están diseñados para engañarle y conseguir que facilite datos de acceso o información financiera, como números de tarjetas de crédito o de la Seguridad Social.

Spear phishing

- Aunque la mayoría de los correos electrónicos de phishing se envían a grandes grupos de personas, hay un tipo de ataque que es más personalizado por naturaleza, el spear phishing. Los correos electrónicos de spear-phishing están dirigidos a una persona, empresa u organización específica. Y a diferencia de los correos electrónicos de phishing más genéricos, los estafadores que los envían dedican tiempo a investigar a sus objetivos. Esta técnica se denomina a veces ingeniería social. Estos delincuentes envían correos electrónicos que parecen proceder de fuentes legítimas.

Clone phishing

- Otro tipo de phishing, el phishing clónico, puede ser uno de los más difíciles de detectar. En este tipo de ataque de phishing, los estafadores crean una versión casi idéntica de un correo electrónico que las víctimas ya han recibido. El correo electrónico clonado se envía desde una dirección que es casi, pero no exactamente, la misma que la dirección de correo electrónico utilizada por el remitente original del mensaje. El cuerpo del mensaje también tiene el mismo aspecto. ¿Cuál es la diferencia? El archivo adjunto o el enlace del mensaje han cambiado. Si las víctimas hacen clic en ellos, les llevarán a un sitio web falso o abrirán un archivo adjunto infectado.

Whaling

- A veces los phishers van a por los objetivos más grandes, las ballenas. Los ataques "balleneros" se dirigen a directores generales, directores de operaciones u otros altos ejecutivos de una empresa. El objetivo es engañar a estas personas poderosas para que entreguen los datos corporativos más confidenciales. Estos ataques son más sofisticados que los ataques generales de phishing y requieren mucha investigación por parte de los estafadores. Suelen basarse en correos electrónicos fraudulentos que parecen proceder de fuentes de confianza dentro de la empresa o de agencias externas legítimas.

Pop-Up Phishing

- El phishing emergente es una estafa en la que los anuncios emergentes engañan a los usuarios para que instalen malware en sus ordenadores o les convencen para que adquieran una protección antivirus que no necesitan. A veces, estos anuncios emergentes utilizan tácticas para asustar. Un ejemplo común de phishing emergente es cuando aparece un anuncio en la pantalla de un usuario advirtiéndole de que su ordenador ha sido infectado y que la única forma de eliminar el virus es instalando un determinado tipo de software antivirus. Una vez que el usuario instala este software, no funciona o, lo que es peor, infecta el ordenador con malware.

A hand holding an open book in a library aisle with tall bookshelves.

Phishing e Ingeniería Social Links

- <https://us.norton.com/internetsecurity-online-scams-what-is-phishing.html>
- <https://www.youtube.com/watch?v=WNVTGTrWcvw>
- <https://www.youtube.com/watch?v=JzoJeJBdhul>
- <https://www.youtube.com/watch?v=Y7zNIEMDmI4>
- <https://www.youtube.com/watch?v=9TRR6IHviQc>
- <https://www.youtube.com/watch?v=BnmneAjVrM4&t>
- <https://www.youtube.com/watch?v=XsOWczwRVuc>
- <https://www.youtube.com/watch?v=j3nE8JQATXo>
- https://www.youtube.com/watch?v=WG8V1_Sj5g0
- <https://www.youtube.com/watch?v=faMyjODoR0>
- <https://www.youtube.com/watch?v=6OHKRA8T18I>
- <https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them>



Huella digital



Que es una huella digital ?

- Una huella digital *-a veces llamada sombra digital o huella electrónica-* es el rastro de datos que dejas al utilizar Internet. Incluye los sitios web que visita, los correos electrónicos que envía y la información que envía en línea. Una huella digital puede utilizarse para rastrear las actividades en línea y los dispositivos de una persona. Los usuarios de Internet crean su huella digital de forma activa o pasiva.
- Cada vez que utilizas Internet, dejas un rastro de información conocido como huella digital. Una huella digital crece de muchas maneras: por ejemplo, publicando en las redes sociales, suscribiéndose a un boletín de noticias, dejando una reseña en línea o comprando en Internet.
- A veces, no siempre es obvio que estás contribuyendo a tu huella digital. Por ejemplo, los sitios web pueden rastrear su actividad instalando cookies en su dispositivo, y las aplicaciones pueden recopilar sus datos sin que usted lo sepa. Una vez que permites que una organización acceda a tu información, podría venderla o compartirla con terceros. Peor aún, tu información personal podría verse comprometida como parte de una filtración de datos.
- A menudo se oyen los términos "activo" y "pasivo" en relación con las huellas digitales

Huella digital activa

- Una huella digital activa es aquella en la que el usuario ha compartido deliberadamente información sobre sí mismo, por ejemplo, publicando o participando en redes sociales o foros en línea. Si un usuario ha iniciado sesión en un sitio web a través de un nombre de usuario o perfil registrado, cualquier publicación que haga formará parte de su huella digital activa. Otras actividades que contribuyen a la huella digital activa son rellenar un formulario en línea -como suscribirse a un boletín- o aceptar cookies en el navegador.

Huella digital pasiva

- Una huella digital pasiva se crea cuando se recopila información sobre el usuario sin que éste sea consciente de ello. Por ejemplo, esto ocurre cuando los sitios web recopilan información sobre cuántas veces los visitan los usuarios, de dónde vienen y su dirección IP. Se trata de un proceso oculto, del que los usuarios pueden no darse cuenta. Otros ejemplos de huellas pasivas son los sitios de redes sociales y los anunciantes que utilizan sus "me gusta", "compartidos" y "comentarios" para elaborar perfiles de los usuarios y ofrecerles contenidos específicos.

A hand holding an open book in a library aisle with tall bookshelves.

Huella Digital Links

- <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>
- https://en.wikipedia.org/wiki/Digital_footprint
- <https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints/>
- <https://www.internetsociety.org/learning/digital-footprints/>
- <https://learnenglishteens.britishcouncil.org/skills/reading/upper-intermediate-b2-reading/your-digital-footprint>
- https://blog-reputationx-com.translate.goog/digital-footprint?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc
- https://techterms.com/definition/digital_footprint
- <https://enhalo.co/360-security/detecting-the-hacker-digital-footprinting>



Herramientas de
seguridad en
internet



Herramientas de seguridad en internet Links

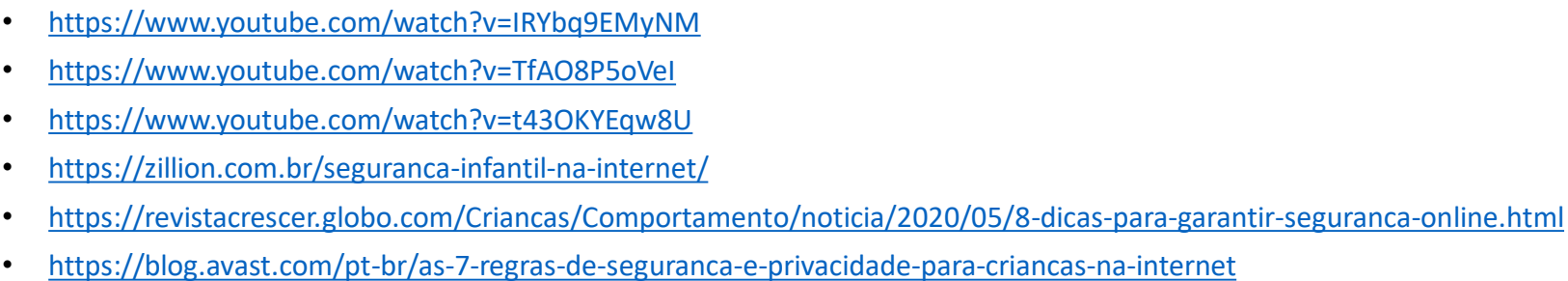
- <https://www.jigsawacademy.com/the-top-5-cyber-security-tools-used-by-organizations/>
- <https://www.techtudo.com.br/tudo-sobre/pc-tools-internet-security.html>
- <https://blog.gigamon.com/2019/06/13/what-is-network-security-14-tools-and-techniques-to-know/>
- <https://www.javatpoint.com/cyber-security-tools>
- <https://theexodusroad.com/10-tools-to-keep-your-kids-safe-online/>
- <https://staysafeonline.org/blog/guide-essential-tools-keep-children-safe-online/>
- <https://internetsafety101.org/Internetsafetytools>
- <https://www.makeuseof.com/tag/7-family-safety-tools-using-kids-online/>
- <https://www.yourlocalsecurity.com/blog/7-awesome-tech-tools-to-keep-kids-safe-online/>
- <https://www.kaspersky.com/resource-center/preemptive-safety/kids-online-safety>
- <https://kidshealth.org/en/parents/net-safety.html>
- <https://sectigostore.com/blog/internet-safety-for-kids-resources-tools-for-parents/>
- <https://br.norton.com/norton-family>
- <https://www.techradar.com/best/parental-control>
- <https://www.pcmag.com/picks/the-best-parental-control-software>
- <https://www.youtube.com/kids/parent-resources/>



Contenido Extra



- <https://www.youtube.com/watch?v=JSx7MBIOnW4>
- <https://www.csa.gov.sg/Programmes/sg-cyber-safe-students/videos/cyber-safety-kids-rsa-security>
- <https://www.youtube.com/watch?v=8tR9P4QX82I>
- <https://www.cisecurity.org/blog/6-educational-cybersecurity-resources-for-kids/>
- <https://www.getcybersafe.gc.ca/en/blogs/cyber-security-kids-how-parents-can-talk-their-children>
- <https://usa.kaspersky.com/resource-center/preemptive-safety/cybersecurity-for-kids>
- <https://www.cisa.gov/sites/default/files/publications/Kids%20Cybersecurity%20Presentation.pdf>
- <https://au.norton.com/internetsecurity-kids-safety-middle-school-kit-a-broader-world-of-cybersecurity-protection.html>
- <https://www.safewise.com/resources/internet-safety-kids/>
- <https://www.outlookindia.com/website/story/outlook-spotlight-cybersecurity-for-kids-its-never-too-early-to-begin/386647>
- <https://www.triptecnologia.com.br/single-post/2019/10/11/10-dicas-de-seguran%C3%A7a-na-internet-para-crian%C3%A7as>



LOONEY TUNES



That's all Folks!